Technical Cybersecurity

The Middle Ages: Malware

1986: Brain Virus

First virus for MS-DOS

- Boot sector virus
- Slowed down floppy drive
- Not malicious, but did cause problems with slow access or removing the last space on a floppy
- Did not infect hard drives!

Not intended to be malicious

- The brothers that wrote it Basit and Amjad Farooq Alvi had a software company, this was supposed to halt piracy

1988: The Morris Worm

Released at MIT

- Written by Robert Morris at Cornell
- Wanted to measure the size of the internet
- Instead implemented a denial of service attack

Spreading

- Multiple vectors: passwords, rsh, mail, finger

Punishment & estimates

- Convicted of a *FELONY*
- Cost estimates based on guesswork, as were damages
- Inspired formation of CERT at CMU

1990: Chameleon Virus

ASIDE: How are viruses detected?

- Back then, only signature based
- Looked for unique aspects of executable

First polymorphic virus

- Changed the bits and bytes of the program
- Inserted junk code
- Based on the Vienna virus

1998: CIH Virus

AKA Chernobyl, spacefiller

- Created by Chen Ing-Hau
- Can erase flash BIOS, required BIOS chip replacement
- Infected Windows 95 systems
- Spread via infected updates from manufacturers, images
- Inserted code into spaces in executables

Lots More!

1989: GHOSTBALL

- First multipartite virus

1995: CONCEPT

- First word macro virus

1999: KAK WORM

- Javascript, exploited an Outlook Express bug

…and hacking?